UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA
Plaintiff,

v. **Case No. 13-CR-155**

JEFFREY FELDMAN
Defendant.

DECISION AND ORDER

The government charged defendant Jeffrey Feldman with receiving and possessing child pornography. Defendant filed motions to compel discovery regarding the computer program ("RoundUp") used by law enforcement to initially detect the alleged presence of child pornography on his computer, and to suppress the evidence gathered pursuant to a subsequently obtained search warrant, arguing that the warrant application failed to establish probable cause and that the affiant misled the issuing magistrate. See Franks v. Delaware, 438 U.S. 154 (1978). The magistrate judge handling pre-trial proceedings in this case received briefs and scheduled oral argument, but on the eve of the argument the parties notified the magistrate judge that they had resolved the case and that the motions would be withdrawn on the filing of a plea agreement. The magistrate judge held a status hearing, confirming this understanding with defendant personally. The parties filed a plea agreement on May 8, 2014, and this court scheduled a plea hearing for June 13, 2014. However, on May 29, 2014, defense counsel filed a letter indicating that defendant was withdrawing from the plea agreement and asking that the motions be set back on the calendar before the magistrate judge.[1] On June 2, 2014, I vacated the plea hearing and referred the case back to the magistrate judge for further action on the motions.

After receiving additional submissions, the magistrate judge concluded that defendant had waived his opportunity to litigate motions. In the alternative, the magistrate judge considered the merits, denying the motion to compel and the request for a Franks hearing, and recommending denial of the motion to suppress.

Defendant objects. I may set aside the magistrate judge's orders on the non-dispositive matters if they are contrary to law or clearly erroneous, Fed. R. Crim. P. 59(a), but my review of the recommendation on the motion to suppress is de novo, Fed. R. Crim. P. 59(b)(3).

I. WAIVER

Defendant notes that prior to the acceptance of his plea he could withdraw from the plea agreement for any reason, see Fed. R. Crim. P. 11(d)(1), and that a plea agreement does not bind the parties until it is approved by the court, see, e.g., United States v. Savage, 978 F.2d 1136, 1137 (9th Cir. 1992). The magistrate judge did not base his waiver conclusion on the executory plea agreement but rather on the explicit statements of defendant and his lawyers that the motions would be withdrawn on the filing of the agreement.

Defendant argues that the magistrate judge's decision to also address the merits signals that he did not really believe waiver applied. It is not uncommon for a judge to reject arguments on both procedural and substantive grounds, particularly when further review is likely. The magistrate judge's thoroughness in this case does not diminish his procedural

[1] It appears that defendant elected not to follow through with the plea after being advised of a possible civil suit by alleged victims of the charged offenses. See 18 U.S.C. § 2255. Such a suit was filed on June 23, 2014, No. 14-C-721, but it has been stayed pending disposition of this criminal case.

ruling.

Defendant further argues that his colloquy with the magistrate judge failed to clearly establish his waiver of motions independent of the plea agreement being heard and accepted by this court. However, he provides no authority in support of the argument, nor does he present any evidence, such as an affidavit from defendant himself, suggesting that he did not understand what he was doing. Cf. United States v. Peterson, 414 F.3d 825, 827-28 (7th Cir. 2005) (rejecting motion to withdraw plea based on affidavit from counsel rather than the defendant). Even assuming, arguendo, that the magistrate judge's colloquy with defendant was insufficient, defendant fails to demonstrate that the right to file motions may not be waived by counsel alone, see Sexton v. French, 163 F.3d 874, 885 (4th Cir. 1998) (listing decisions that must be made by the defendant and those which can be made by counsel, with motions falling in the latter category), or that "withdrawal" does not equal waiver, see United States v. Tichenor, 683 F.3d 358, 363 (7th Cir. 2012) (collecting cases). Defendant contends that counsel mis-spoke in indicating that the motions would be withdrawn on filing of the plea agreement (presenting affidavits from counsel to that effect), and that offering an unconditional waiver without the plea agreement being accepted by the court would constitute ineffective assistance of counsel. It suffices to note that based on the information before me it was defendant who made the decision not to follow through with the plea agreement, foregoing its benefits, based on the possible civil suit, even though the agreement included a paragraph advising defendant that restitution for the offense was mandatory and that imposition of restitution would not preclude the filing of a civil suit. (Plea Agreement [R. 40] ¶ 26.)

Finally, defendant argues that, to the extent the magistrate judge deemed the defense to be asking for more time to file motions, his discovery of the possible civil remedies under 18

U.S.C. § 2255 constitutes "good cause" for the acceptance of an untimely motion. See Fed. R. Crim. P. 12(c)(3).[2] Defendant provides no authority for this argument, and courts have held that withdrawal of a plea does not entitle a defendant to an extension of the pre-trial motion deadline. United States v. Walden, 625 F.3d 961, 966 (6th Cir. 2010).

In sum, defendant fails to establish clear error in the magistrate judge's waiver determination.[3] In any event, like the magistrate judge, I will also address the merits.

II. MERITS

A. Motion to Suppress

1. Legal Standards

In resolving a motion to suppress evidence gathered pursuant to a search warrant, I first ask whether the affidavit provided the issuing magistrate with a "substantial basis" to find probable cause. United States v. Koerth, 312 F.3d 862, 866 (7th Cir. 2002) (citing Illinois v. Gates, 462 U.S. 213, 238 (1983)). Probable cause is far short of certainty; it requires only a probability or substantial chance of criminal activity, not an actual showing of such activity or even a probability that exceeds 50 percent. United States v. Seiver, 692 F.3d 774, 777 (7th Cir. 2012). Determining whether probable cause exists requires a common-sense analysis of the

[2] Rule 12 was revised effective December 1, 2014, with the "good cause" provision for untimely motions being relocated from sub.(e) to sub. (c).

[3] Defendant argues that the government did not offer and the magistrate judge did not identify any prejudice to the government based on these events. In its response to the objections, the government indicates that in an effort to resolve the discovery dispute it flew in an FBI representative from Washington to provide a demonstration for the defense team, but that demonstration was canceled when the parties reached an agreement to resolve the case. The government contends that these efforts belie any claim that the government did not rely on defendant's waiver. In reply, defendant characterizes this argument as a red herring, but he does not dispute the underlying facts.

facts available to the judicial officer who issued the warrant. United States v. Carroll, 750 F.3d 700, 703 (7th Cir. 2014). When a search is authorized by a warrant, deference is owed to the issuing magistrate’s conclusion that there is probable cause. Id. at 703-04.

If the defendant demonstrates that the affidavit failed to establish probable cause, the burden shifts to the government to show that the officers could have relied in “good faith” on the magistrate’s decision to issue the warrant. Koerth, 312 F.3d at 868 (citing United States v. Leon, 468 U.S. 897, 924 (1984)). An officer’s decision to obtain a warrant is prima facie evidence that he was acting in good faith. Id. The defendant may rebut this prima facie case by presenting evidence that the magistrate wholly abandoned his judicial role, or that the officer submitted an affidavit so lacking in indicia of probable cause as to render official belief in its existence unreasonable. Id. Under the latter theory, the defendant must show that courts have clearly held that a materially similar affidavit previously failed to establish probable cause under facts that were indistinguishable from those presented in the case at hand, or the affidavit is so plainly deficient that any reasonably well-trained officer would have known that his affidavit failed to establish probable cause and that he should not have applied for the warrant. Id. at 869.

The good faith exception does not apply if the affiant misled the issuing magistrate. United States v. Harris, 464 F.3d 733, 740 (7th Cir. 2006); see also Franks, 438 U.S. at 171 (holding that although a presumption of validity applies to search warrants, the defendant may in some circumstances be able to challenge the veracity of the application). In order to obtain a so-called Franks hearing, the defendant must make a “substantial preliminary showing” that the warrant application contained a materially false statement made by law enforcement with deliberate or reckless disregard for the truth and that the false statement was necessary for the finding of probable cause. United States v. Williams, 718 F.3d 644, 649 (7th Cir. 2013). Under Franks, evidence recovered from a search must be suppressed if the defendant is able to prove by a preponderance of the evidence that (1) the affidavit contained material false statements or omissions, (2) these false statements or omissions were made with deliberate or reckless disregard for the truth, and (3) these false statements or omissions were necessary to a finding of probable cause. Id.

2. Analysis

The search warrant in this case issued based on the January 22, 2013, affidavit of FBI Special Agent Brett Banner.[4] (R. 27-2 at 1-2.) After discussing his credentials and training, and explaining certain technical terms (id. at 2-3), Banner set forth the following information specific to this case.

Between June 10, 2012, and July 23, 2012, an FBI online covert employee ("OCE") conducted numerous online investigations to identify individuals possessing and sharing child pornography using the eDonkey and KAD peer-to-peer ("P2P") networks. The OCE used a P2P file sharing program, which scanned both networks simultaneously and has been enhanced to ensure that downloads occur only from a single selected source.[5] (Id. at 4 ¶ 7.) During those investigations, the OCE searched for suspected child pornography files and

[4] In his objections, defendant nitpicks at the magistrate judge's statement of facts contained in the warrant application. (R. 53 at 9-10.) He identifies no significant misstatements. In any event, I have reviewed the application de novo and summarize it in the following text.

[5] Earlier in his affidavit, Banner explained that, typically, users of a P2P network receive a selected file from numerous sources, with the pieces reassembled to complete the file in the local computer. (Id. at 3 ¶ 6.f.)

identified a particular IP address[6] on the KAD network which had suspected child pornography files available for distribution. Specifically, this IP address responded to the OCE's queries for 17 suspected child pornography hash values.[7] (Id. at 4 ¶ 8.)

Banner averred that during the dates listed, the target IP address was registered to Time Warner/Road Runner and assigned to a physical address in Milwaukee, Wisconsin. (Id. at 4 ¶ 9.) On September 6, 2012, the aforementioned suspected child pornography hashes were submitted to the National Center for Missing and Exploited Children ("NCMEC") for preliminary identification. NCMEC advised that five of them "matched known child pornography victims." (Id. at 5 ¶ 10.) The affidavit then specifically described two of those files. (Id.) Banner averred that the "remaining hashes were identified as 'Recognized,' which meant they had been previously submitted to NCMEC as suspected child pornography by law enforcement." (Id. at 5 ¶ 11.)

While conducting the investigation, the OCE attempted without success to conduct single source downloads of the suspected child pornography from the target IP address. The OCE noted that the IP address had been given a "low ID" designation on the KAD network, which, for technical reasons, may have prevented the single source download. (Id. at 5 ¶ 12.)

On September 7, 2012, Time Warner responded to a subpoena requesting subscriber information for the target IP address, identifying defendant at a physical address in West Allis,

[6] Banner explained that an IP address is a unique numeric address assigned to every computer attached to the internet. (Id. at 2 ¶ 6.a.)

[7] Banner explained that a hash algorithm value is assigned to each file being shared on a P2P network. "Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their file names." (Id. at 3 ¶ 6.f.)

Wisconsin. (Id. at 5-6 ¶ 13.) On September 13, 2012, agents went to the physical address to conduct surveillance and determine if there was a wireless connection that could be associated with this residence. A check of the available wireless connections revealed that there were several secured wireless connection points that could be associated with the residence. There were no unsecured wireless connection points found at this location, indicating that the suspect's wireless connection was secured. (Id. at 6 ¶ 14.) On December 6, 2012, Banner viewed a law enforcement commercial data base and learned that defendant had lived at the West Allis address since 1997. (Id. at 6 ¶ 15.) State records further revealed that defendant had vehicles registered to him at this address. (Id. at 6 ¶ 16.)

Based on these facts, Banner averred that there was probable cause to believe that evidence of violations of 18 U.S.C. § 2252A was located at defendant's West Allis residence. (Id. at 9 ¶ 23.) Magistrate Judge Callahan issued the warrant on January 22, 2013. (Case No. 13-mj-421.)

Banner's affidavit supplied a substantial basis for a finding of probable cause. The OCE, while investigating P2P networks, identified an IP address with suspected child pornography files available for distribution. Courts have upheld such investigations, as P2P users have no expectation of privacy in files available for sharing. E.g., United States v. Borowy, 595 F.3d 1045, 1048 (9th Cir. 2010); United States v. Stults, 575 F.3d 834, 843 (8th Cir. 2009). The OCE was unable to download the files in this case, but s/he did identify them by hash values. Courts have found hash values sufficiently reliable, even in the absence of a direct download. See, e.g., United States v. Thomas, No. 12-CR-27, 2013 U.S. Dist. LEXIS 159914, at *63-64 (D. Vt. Nov. 8, 2013) ("Defendants cite to no authority for their claim that hash values are inherently unreliable or that a direct download of the file is necessary to establish probable cause. Courts have routinely found otherwise."); id. at *68 ("Even without a direct download, courts have consistently found probable cause exists when an IP address that appears to have accessed child pornography can be traced to an identifiable residence."); United States v. Wunderli, No. 11 CR 538, 2012 U.S. Dist. LEXIS 57964, at *16 (E.D. Mo. Mar. 27, 2012) (finding that hash values sufficiently identified files as child pornography), adopted, 2012 U.S. Dist. LEXIS 57963 (E.D. Mo. Apr. 25, 2012); see also United States v. Collins, 753 F. Supp. 2d 804, 807, 810-11 (S.D. Iowa 2010) (finding sufficient corroboration where law enforcement compared SHA-1 values of images on the defendant's computer to values of images in database of known child pornography);[8] United States v. Harner, No. 09-CR-155, 2009 U.S. Dist. LEXIS 78742, at *6-7 (D. Minn. Sept. 1, 2009) (finding that probable cause would likely exist, even if the officer did not view files from the defendant's computer, based on comparison of hash values to database of suspect files). Finally, the agents confirmed that the hash values matched known child pornography by submitting them to NCMEC and viewing two of the files associated with the hash values, providing a detailed description of those two files. See Thomas, 2013 U.S. Dist. LEXIS 159914, at *63 (noting that law enforcement

[8] Defendant attempts to distinguish Collins as a Franks case. Much like this case, the defendant in Collins initially challenged the probable cause basis for the warrant and then sought a Franks hearing. Id. at 808. The primary basis for the Franks argument in Collins was that the officer-affiant failed to disclose reliability problems with the computer program the government used, id., again much like this case. In rejecting that argument, the court noted that even if the issuing magistrate had been told of the possible margin of error in the program probable cause would still exist. Id. at 811. In making this finding, the court noted that the officers corroborated what they had learned through the program by "comparing the SHA-1 values of the images on Defendant's computer to the SHA-1 values of images in DCI's library." Id. at 810. In sum, Collins is very much analogous to the present case.

examined images associated with the identified hash values).[9]

In his objections, defendant contends that no court has found that a target computer responding to hash value queries, without some further corroboration that the target computer likely contains child pornography, is sufficient to establish probable cause for a search warrant. He points to my decision in United States v. Case, where I indicated, in response to the defendant's complaint about the use of an automated law enforcement program, "This is not a situation where a computer program downloaded material believed to be contraband (based on, say, a keyword search or hash values) and no human being looked at the material before a warrant was sought." No. 13-CR-120, 2014 U.S. Dist. LEXIS 34460, at *13 (E.D. Wis. Mar. 17, 2014). In this case, the agents did not rely on the target computer's response to the hash value query alone; they submitted the hash values to the NCMEC for confirmation, viewed two of the offered files, and provided the magistrate judge with a detailed description of the contents of those two files.[10] Defendant attempts to distinguish Thomas, arguing that unlike

[9] While the warrant affidavit does not explicitly state that the agents personally viewed the two files described therein, that is a fair inference. See United States v. Carmel, 548 F.3d 571, 575 (7th Cir. 2008) ("Judges may draw reasonable inferences from the totality of the circumstances in determining whether probable cause exists to issue a warrant.") (internal quote marks omitted). Defendant fails to explain how Banner could have provided a detailed description of these files had agents not viewed them. I do not in making this finding rely on the supplemental affidavit Banner submitted along with the government's opposition to the motion to suppress (R. 30-2 at 3-4 ¶ 20), in which he makes this clear. See United States v. Peck, 317 F.3d 754, 755 (7th Cir. 2003) ("When an affidavit is the only evidence presented to a judge in support of a search warrant, the validity of the warrant rests solely on the strength of the affidavit.").

[10] Defendant cites United States v. Miknevich, 638 F.3d 178, 183 (3d Cir. 2011), for the proposition that an "insufficiently detailed or conclusory description" of alleged child pornography images would not satisfy the Fourth Amendment. In the present case, Banner provided a detailed description of two videos. See id. (noting that "either the actual production of the images, or a sufficiently detailed description of them" would satisfy the Fourth Amendment's probable cause requirement). I also note that while the Miknevich court stated

in his case the officers there physically examined the images associated with the identified hash values. As discussed above, the instant warrant application, fairly read, establishes the same. In any event, defendant concedes that the odds of two different files having the same hash value are infinitesimal.[11]

Defendant argues that, unlike the program used in Thomas, RoundUp has the ability to infiltrate private spaces on the target computer. He offers no evidence of that. While the affidavit from his expert references remote "tagging," he makes no claim that such tagging occurred in his case. Nor does the affidavit affirmatively contend that the program invades non-shared space to search for evidence. (See R. 25-1 at 6 ¶ 22 – "It can't be confirmed if the software has access to, or writes information in other non-shared areas of the remote client.") Relying on his expert, defendant further contends that it may be possible for hash values to be present on a computer without the computer having any significant portion of the file present on it (like having the table of contents of a book without having any of the chapters). But this possibility does not defeat probable cause, which requires only a substantial chance that a search will turn up evidence of criminal activity. As the Miknevich court stated:

> We recognize that file names are not always a definitive indication of actual file content and, therefore, only after downloading and viewing a particular file can one know with certainty whether the content of the file is consistent with its designated name. However, certainty has no part in a probable cause analysis. On the contrary, probable cause requires only a probability or substantial chance

that the "better practice" would be to append the images or provide a sufficient description, in the case before it concluded that the "magistrate could have drawn a reasonable inference of the file's contents based on its highly descriptive name and SHA1 value." Id. at 184. The holding of Miknevich thus undermines defendant's position that only physical viewing of the file will suffice, and that an issuing magistrate cannot rely on hash values.

[11] Nor does defendant address the agents' efforts to corroborate the information gathered through RoundUp by submitting the hash values to the NCMEC.

> of criminal activity, not an actual showing of such activity.

638 F.3d at 184-85 (internal citations and quote marks omitted).

Even if the application failed to establish probable cause, the agents could have relied in good faith on the magistrate's decision to issue the warrant.[12] Defendant makes no claim that Magistrate Judge Callahan simply rubber stamped the application; he cites no case finding a materially similar application insufficient; and he makes no effort to show that the affidavit was so plainly deficient that any reasonably well-trained officer would have known that it failed to establish probable cause. Instead, he argues that good faith does not apply because the affiant was dishonest or reckless.

However, defendant points to no false statements in or material omissions from the affidavit. Instead, he argues that RoundUp exploits known weaknesses in the P2P program and is able to locate information (including hash histories) deleted or moved so as to prevent file sharing. In support of this claim, he cites an article which states that, "the exact extent to which can [sic] investigators can exploit a network protocol to gather information remotely is unsettled law." (R. 34-1 at 3, cited in R. 53 at 21.) He contends that the "phrase 'exploiting a network protocol' is just techno-babble for writing a program that invades an otherwise non-shared portion of a computer." (R. 53 at 22.) He concludes that the government essentially developed a virus that allowed it to access all of the data on a P2P user's computer, which it failed to disclose to the issuing magistrate. (R. 53 at 22; see also R. 58 at 11, citing R. 34-1 at 3, claiming that the "developers of RoundUp themselves have stated that it exploits weaknesses in peer-to-peer networks and that the exploitation of those weaknesses may

[12] The government raised good faith before the magistrate judge.

violate Kyllo.")

As I noted in rejecting the same contention in Case, defendant's argument regarding invasion of non-shared spaces fits better under the Murray/Markling framework, see 2014 U.S. Dist. LEXIS 34460, at *6 (citing Murray v. United States, 487 U.S. 533, 542 (1988); United States v. Markling, 7 F.3d 1309, 1315 (7th Cir. 1993)), than it does under Franks. In any event, defendant presents no evidence that RoundUp does what he claims, much less that it did so in this investigation. As I noted in Case, there is no support for these claims in the articles submitted. Id. at *9-12. For instance, the article defendant cites in his objections discusses digital forensics in general; it says nothing about RoundUp in particular. Further, the authors of this article clearly state that pre-warrant evidence must be in plain view, which in this context would mean the shared portion of the computer, in order for it to be used. (R. 34-1 at 2.) Defendant presents no non-speculative basis for holding a hearing, either to explore the legality of the government's pre-warrant investigation or the veracity of the affiant. See United States v. Curlin, 638 F.3d 562, 564 (7th Cir. 2011).

For these reasons and those stated by the magistrate judge, the motion to suppress will be denied. I also decline to overturn the magistrate judge's denial of a Franks hearing. As discussed above and in the magistrate judge's order, defendant fails to make a substantial preliminary showing that the application included false or misleading statements, or material omissions. Nor does defendant offer direct evidence of the affiant's state of mind or inferential evidence suggesting deliberate deception or reckless disregard. See United States v. Souffront, 338 F.3d 809, 822 (7th Cir. 2003).

B. Motion to Compel

The magistrate judge denied defendant's motion to compel disclosure of the RoundUp program, its manual and protocols, and its technical specifications, concluding that defendant failed to show that this information was "material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E). The magistrate judge noted that while the government used RoundUp to identify defendant as a suspect, the receipt/possession charges against him are based on the evidence recovered from his home pursuant to the search warrant. This, the magistrate judge concluded, distinguished United States v. Budziak, 697 F.3d 1105, 1111-13 (9th Cir. 2012), where the court required disclosure of the government's program; in Budziak, the defendant was charged with child pornography distribution based on images the government obtained through use of the program.

In his objections, defendant argues against any distinction between defenses raised by motion and those raised at trial. However, he cites no specific authority in support of his contention, and some courts have rejected it. See, e.g., United States v. Hunt, No. 2:11-CR-441, 2013 U.S. Dist. LEXIS 136135 , at *3-4 (E.D. Cal. Sept. 18, 2013) (citing United States v. Armstrong, 517 U.S. 456, 462 (1996), which employed a "shield and sword" metaphor in discussing Rule 16, and concluding that information sought to bolster a motion to suppress related to a "sword" claim).

In any event, defendant fails to identify any specific defenses that discovery of the RoundUp materials could help him develop, whether presented by pre-trial motion or at trial. He points to his expert's affidavit discussing certain features of RoundUp, which he argues may violate the Fourth Amendment. However, he fails to explain how his speculation about "tagging" or other possible program capabilities would support his motion to suppress.[13] He

[13] In his reply brief, defendant claims that RoundUp may be able to access files or other information in the non-shared portions of a target computer. (R. 58 at 11, citing R. 25-1 at 4,

then posits several possible uses of the information at trial, but most depend on the government's presentation of RoundUp acquired evidence in its case-in-chief.[14] He references a possible entrapment defense, but he offers no evidence that the government used the program to insert child pornography or associated hash values onto his computer.[15] In sum, defendant fails to show that the magistrate judge clearly erred in denying his motion to compel.

III. CONCLUSION

THEREFORE, IT IS ORDERED that defendant's objections are overruled, the magistrate judge's recommendation is adopted, and defendant's motion to suppress (R. 26) is **DENIED**.

IT IS FURTHER ORDERED that this case is scheduled for **STATUS** on **Monday, January 26, 2015, at 10:45 a.m.**

Dated at Milwaukee, Wisconsin, this 19th day of January, 2015.

/s Lynn Adelman
LYNN ADELMAN
District Judge

¶ 15.) In ¶ 15 of his affidavit, defendant's expert discusses "tagging." As I discussed in Case, tagging involves the insertion of data into a remote computer. These tags can later be recovered from the storage media after the computer is seized pursuant to a search warrant (not unlike marked bills used in a controlled drug buy) and then used to link the remote observations to the particular suspect and his computer. In sum, the technique allows law enforcement to positively identify the seized computer as the same one that was investigated remotely. 2014 U.S. Dist. LEXIS 34460, at *5-6 n.2. Defendant's expert contends that when this occurs the tag is stored in a non-shared part of the computer. However, he makes no claim that RoundUp allows law enforcement to access files in the non-shared part of a computer.

[14] There is no indication that the OCE is a transactional witness under Roviaro. See United States v. Jefferson, 252 F.3d 937, 941-42 (7th Cir. 2001).

[15] In its response to the objections, the government notes that defendant does not explain how such a defense could possibly account for the thousands of child pornography files he allegedly collected long before law enforcement interacted with his computer.